UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA,	Case No. 1:23-cr-97 (DJN)
v.	Hon. David J. Novak
MOHAMMED AZHARUDDIN CHHIPA,	
Defendant.	

THE GOVERNMENT'S UNCLASSIFIED BRIEF IN OPPOSITION TO THE DEFENDANT'S MOTION TO DISCLOSE AND SUPPRESS FISA MATERIALS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

U.S. CONSTITUTION

FEDERAL STATUTES

OTHER AUTHORITIES

I. INTRODUCTION

The Government files this unclassified brief opposing defendant Mohammed Chhipa's (Chhipa) Motion to Suppress the Content of Unlawful Electronic Surveillance and the Fruit Thereof, and to Compel Disclosure of all Surveillance Material (ECF No. 111, hereinafter "Mot.").[1] Chhipa seeks (1) suppression of all evidence obtained or derived under the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801, *et seq.*; (2) suppression of all evidence obtained or derived pursuant to 50 U.S.C. § 1881a (Section 702) of the FISA Amendments Act (FAA); and (3) disclosure of the FISA applications, orders, Section 702 material, querying information, and information on other government surveillance programs used to collect his information. Mot. at 1.

Chhipa's motion triggered this Court's review of the FISA application(s), order(s), and related materials (*i.e.*, the FISA materials)[2] related to the FISA-authorized electronic surveillance and physical search at issue in this case to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search conformed with an order of authorization or approval.[3] FISA specifies:

> [W]henever a motion is made pursuant to subsection (e) . . . to discover or obtain applications or orders or other materials relating to electronic surveillance [or physical search] or to discover, obtain, or suppress

---

[1] A classified version of this brief has been filed with the Classified Information Security Officer. The pagination and footnote numbering in this unclassified brief differ from the classified version due to redactions.

[2] **[CLASSIFIED INFORMATION REDACTED]**

[3] The FISA provisions that address electronic surveillance are found at 50 U.S.C. §§ 1801-1812; those that address physical search are found at 50 U.S.C. §§ 1821-1829. These two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision.

> evidence or information obtained or derived from electronic surveillance [or physical search] under this Act, the United States district court . . . shall, . . . if the Attorney General[4] files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance [or search] as may be necessary to determine whether the surveillance [or search] of the aggrieved person was lawfully authorized and conducted.

50 U.S.C. §§ 1806(f), 1825(g). The Government is filing herewith such an affidavit.[5] Accordingly, this Court must conduct an *in camera, ex parte* review of the FISA materials relevant to Chhipa's motion consistent with 50 U.S.C. §§ 1806(f) and 1825(g).[6]

As discussed below, this Court's *in camera, ex parte* review will show that: (1) suppression of the FISA information is unwarranted because the electronic surveillance and physical search at issue were lawfully authorized and conducted in compliance with FISA; (2) Chhipa lacks standing to suppress any putative information obtained or derived under Section 702, and accordingly did not receive notice of the Government's intent to use acquisitions obtained pursuant to Section 702; and (3) disclosure of the FISA materials and the Government's classified submission(s) to Chhipa is not authorized because this Court can accurately determine the legality of the FISA-authorized electronic surveillance and physical search without disclosing the FISA materials or portions thereof.

---

[4] As defined in FISA, "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General for National Security (AAG/NS). *See* 50 U.S.C. §§ 1801(g), 1821(1). Attorney General Eric H. Holder, Jr., made such a designation on April 24, 2009.

[5] The Government is filing both publicly and as an exhibit in the Sealed Appendix the Declaration and Claim of Privilege, an affidavit executed by the AAG/NS. *See* Sealed Ex. 1.

[6] **[CLASSIFIED INFORMATION REDACTED]**

A. BACKGROUND

In May 2023, a grand jury in this district returned an indictment charging Chhipa with five counts of providing, attempting to provide, and conspiring to provide material support to the Islamic State of Iraq and al-Sham (ISIS), in violation of 18 U.S.C. §§ 2339B and 2.[7]

[CLASSIFIED INFORMATION REDACTED]

On August 18, 2023, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the Government provided notice to this Court and Chhipa that it intended to offer into evidence, or otherwise use or disclose, information obtained or derived from electronic surveillance and physical search conducted pursuant to FISA. ECF No. 50.

[CLASSIFIED INFORMATION REDACTED]

On June 3, 2024, Chhipa filed his motion seeking disclosure of the FISA materials and suppression of the FISA information. ECF No. 111.

[CLASSIFIED INFORMATION REDACTED]

B. OVERVIEW OF THE FISA AUTHORITIES AT ISSUE

[CLASSIFIED INFORMATION REDACTED]

1. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

2. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

[7] On August 15, 2024, a grand jury in this district returned a superseding indictment charging Chhipa with these same counts. *See* ECF No. 117.

The various findings required under FISA to authorize electronic surveillance or physical search, and the Government's submissions to the FISC addressing those requirements in the docket(s) at issue, are discussed in detail below.

II. THE FISA PROCESS

To aid this Court's review, this brief provides an overview of the FISA process. It covers the FISC's and the Attorney General's roles prescribed in FISA, the requirements to apply for a FISA order to conduct electronic surveillance or physical search, the findings the FISC must make in issuing such an order, and the procedures and standards governing a district court's review of FISA authorities when evidence obtained or derived therefrom is used in criminal proceedings. Not every part of FISA discussed below is at issue, and this brief notes where certain aspects of FISA are not directly implicated in this matter. This brief still discusses those other aspects to give context for this Court's review of the surveillance and search at issue.

A. OVERVIEW OF FISA

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States district judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical search when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court of Review (FISC of Review), which is composed of three United States district or circuit judges who are designated by the Chief Justice. *Id.* § 1803(b).

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance and/or physical search in the United States

when a significant purpose is the collection of foreign intelligence information.[8] 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, foreign intelligence information means:

> (1) information that relates to, and if concerning a United States person[9] is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

Id. § 1801(e); *see also id.* § 1821(1) (adopting the definitions from 50 U.S.C. § 1801). Except for emergency authorizations, FISA requires the Government to obtain a court order before it conducts any electronic surveillance or physical search.

FISA provides that the Attorney General may authorize the emergency employment of electronic surveillance and physical search if the Attorney General:

> (A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance [or physical search] to obtain foreign intelligence information before an order authorizing such surveillance [or physical search] can with due diligence be obtained;
>
> (B) reasonably determines that the factual basis for the issuance of an order under this title to approve such electronic surveillance [or physical search] exists;

---

[8] **[CLASSIFIED INFORMATION REDACTED]**

[9] **[CLASSIFIED INFORMATION REDACTED]**

> (C) informs, either personally or through a designee, a judge having jurisdiction under [50 U.S.C. § 1803] at the time of such authorization that the decision has been made to employ emergency electronic surveillance [or physical search]; and
>
> (D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than 7 days after the Attorney General authorizes such electronic surveillance [or physical search].

50 U.S.C. §§ 1805(e)(1), 1824(e)(1).[10] Emergency electronic surveillance or physical search must comport with FISA's minimization requirements, which are discussed below. *Id.* §§ 1805(e)(2), 1824(e)(2).[11]

B. THE FISA APPLICATION

An application to conduct electronic surveillance pursuant to FISA must contain, among other things:

> (1) the identity of the federal officer making the application;
>
> (2) the identity, if known, or a description of the specific target of the electronic surveillance;
>
> (3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power,

---

[10] **[CLASSIFIED INFORMATION REDACTED]**

[11] If the FISC does not issue an order authorizing the electronic surveillance or physical search, emergency surveillance or search must terminate when the information sought is obtained, when the FISC denies an application for an order, or after the expiration of seven days from the time of the emergency employment, whichever is earliest. *See* 50 U.S.C. §§ 1805(e)(3), 1824(e)(3). Moreover, if no FISC order is issued, absent a showing of good cause, the FISC shall cause to be served on any U.S. person named in the application, and others in the FISC's discretion, notice of the fact of the application, the period of the surveillance or search, and the fact that during the period information was or was not obtained. *See id.* § 1806(j); *see also id.* § 1825(j)(1) (physical search). In addition, if no FISC order is issued, neither information obtained nor evidence derived from the emergency electronic surveillance or physical search may be disclosed in any court or other proceeding, and no information concerning a U.S. person acquired from the electronic surveillance or physical search may be used in any other manner by Federal officers or employees without the person's consent, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm. *See id.* §§ 1805(e)(5), 1824(e)(5).

> and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (4) a statement of the proposed minimization procedures;
>
> (5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
>
> (6) a certification, discussed below, of a high-ranking official;
>
> (7) a summary of the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;
>
> (8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and
>
> (9) the proposed duration of the electronic surveillance.

50 U.S.C. § 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance, except that an application to conduct a physical search must also contain a statement of the facts and circumstances justifying an applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that each "premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from" the target. *Id.* § 1823(a)(1-8), (a)(3)(B), (C).

1. The Certification

An application to the FISC for a FISA order must include a certification from a high-ranking Executive Branch official with national security responsibilities that:

> (A) the certifying official deems the information sought to be foreign intelligence information;
>
> (B) a significant purpose of the surveillance is to obtain foreign intelligence information;

> (C) such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and
>
> (E) includes a statement of the basis for the certification that –
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6); *see also id.* § 1823(a)(6).

As originally enacted, FISA required that a high-ranking member of the Executive Branch of Government certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act).[12] The USA PATRIOT Act changed FISA so that a high-ranking official must now certify that the acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance or search. *See id.* §§ 1804(a)(6)(B), 1823(a)(6)(B).

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting U.S. persons that was obtained through FISA-authorized electronic surveillance or physical search, including persons who are not the targets of the FISA authorities. FISA requires that such minimization procedures be:

[12] Pub. L. No. 107-56, 115 Stat. 272 (2001).

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. §§ 1801(h)(1), 1821(4)(A).

Minimization procedures also include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." *Id.* §§ 1801(h)(3), 1821(4)(c).

[CLASSIFIED INFORMATION REDACTED]

3. Attorney General's Approval

FISA also requires that the Attorney General approve applications for electronic surveillance and/or physical search before they are presented to the FISC, "based upon [a] finding that it satisfies the criteria and requirements" in FISA. *Id.* §§ 1804(a), 1823(a).

C. THE FISC'S ORDERS

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance and/or physical search only upon finding, among other things, that:

> (1) the application has been made by a Federal officer and has been approved by the Attorney General;
>
> (2) there is probable cause to believe that (A) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power, or that the premises or property to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power;

> (3) the proposed minimization procedures meet the statutory requirements set forth in section 1801(h) (electronic surveillance) and section 1821(4) (physical search);
>
> (4) the application contains all of the statements and certifications required by section 1804 (electronic surveillance) or section 1823 (physical search); and
>
> (5) if the target is a United States person, the certifications are not clearly erroneous.

50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

FISA defines "foreign power" to mean—

> (1) a foreign government or any component, thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> (4) a group engaged in international terrorism or activities in preparation therefor;
>
> (5) a foreign-based political organization, not substantially composed of United States persons;
>
> (6) an entity that is directed and controlled by a foreign government or governments; or
>
> (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

Id. § 1801(a)(1)-(7); *see also id.* § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"Agent of a foreign power" means—

> (1) any person other than a United States person, who—
>
> > (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4), irrespective of whether the person is inside the United States;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances indicate that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore [sic];

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraphs (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraphs (A), (B), or (C).

50 U.S.C. § 1801(b)(1), (2); *see also id.* § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

FISA specifies that no U.S. person may be considered a foreign power or an agent of a foreign power based solely on First Amendment protected activities. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). Although First Amendment protected activities cannot form the sole basis for FISA-authorized electronic surveillance or physical search, the FISC may consider them if other activity indicates the target is an agent of a foreign power. *United States v. Rosen*, 447 F. Supp. 2d 538, 548-49 (E.D. Va. 2006); *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999).

The FISA application must establish probable cause to believe the target is acting as an agent of a foreign power at the time of the application. *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000). However, in determining whether probable cause exists, FISA allows a judge to "consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b), 1824(b).

If the FISC makes all necessary findings and concludes the FISA application meets the statutory provisions, the FISC issues an *ex parte* order authorizing the electronic surveillance and/or physical search requested in the application. *Id.* §§ 1805(a), 1824(a). The order must:

> (1) . . . specify—
>
> > (A) the identity, if known, or a description of the specific target of the [collection];
> >
> > (B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known [and/or of each of the premises or properties to be searched];
> >
> > (C) the type of information sought to be acquired and the type of communications or activities to be subjected to the [electronic] surveillance [and/or the type of information, material, or property to be seized, altered, or reproduced through the physical search];

> (D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance [and/or a statement of the manner in which the physical search will be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search]; and
>
> (E) the period of time during which the electronic surveillance is approved [and/or the period of time during which physical searches are approved; and]
>
> (2) . . . direct—
>
> (A) that the minimization procedures be followed . . . .

50 U.S.C. §§ 1805(c)(1), (2)(A), 1824(c)(1), (2)(A).

Initial FISC approval for electronic surveillance and/or physical search targeting a U.S. person may be approved for up to 90 days, and those targeting a non-U.S. person may be approved for up to 120 days. *Id.* §§ 1805(d)(1), 1824(d)(1). The FISC may renew such approval, but only if the Government submits another application that complies with FISA's requirements. A renewal for electronic surveillance or physical search targeting a U.S. person may be approved for up to 90 days, and one targeting a non-U.S. person may be approved for up to one year.[13] *See id.* §§ 1805(d)(2), 1824(d)(2).

III. THE DISTRICT COURT'S REVIEW OF FISC ORDERS

FISA authorizes the use of information obtained or derived from FISA-authorized electronic surveillance or physical search in a criminal prosecution, provided that the Government obtains advance authorization from the Attorney General, *see id.* §§ 1806(b), 1825(c), and then gives proper notice to the court and to each aggrieved person against whom the

[13] The FISC retains the authority to review, before the end of the authorized period of electronic surveillance or physical search, the Government's compliance with the requisite minimization procedures. *See* 50 U.S.C. §§ 1805(d)(3), 1824(d)(3).

information is to be used.[14] *See* 50 U.S.C. §§ 1806(c)-(d), 1825(d)-(e). Upon receiving notice, an aggrieved person against whom the information is to be used may move to suppress the use of the FISA information on two grounds: (1) that the information was unlawfully acquired; or (2) that the electronic surveillance or physical search was not made in conformity with an order of authorization or approval. *Id.* §§ 1806(e), 1825(f). In addition, FISA contemplates that a defendant may file a motion or request under any other statute or rule of the United States to discover or obtain applications, orders, or other materials relating to electronic surveillance or physical search, *i.e.*, the FISA materials. *Id.* §§ 1806(f), 1825(g).

When a defendant moves to suppress FISA information under 50 U.S.C. §§ 1806(e) or 1825(f), or seeks to discover the FISA materials under some other statute or rule, the motion or request is evaluated using FISA's probable cause standard, discussed below, and not the probable cause standard applicable to criminal warrants. *See, e.g., United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *United States v. El-Mezain*, 664 F.3d 467, 564 (5th Cir. 2011); *United States v. Duka*, 671 F.3d 329, 336-37 (3d Cir. 2011).

A. THE REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

In assessing the legality of FISA-authorized electronic surveillance and/or physical search, the district court:

> shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm

---

[14] An "aggrieved person" is defined as the target of electronic surveillance or "any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), as well as "a person whose premises, property, information, or material is the target of physical search" or "whose premises, property, information, or material was subject to physical search." *Id.* § 1821(2). Chhipa is an "aggrieved person" under FISA, and as noted above, the Government provided notice of his aggrieved person status and of its intent to use FISA-obtained or -derived information against him at trial.

> the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.[15]

50 U.S.C. §§ 1806(f), 1825(g). When the AAG/NS files such an affidavit or declaration, as he did here, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance [or physical search] *only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]*." *Id.* §§ 1806(f), 1825(g) (emphasis added).

Thus, a district court's discretion to disclose FISA materials to an aggrieved defendant is limited, and such disclosure is unwarranted unless the court cannot accurately determine the legality of the FISA authorities even after reviewing the Government's *in camera* and *ex parte* submissions. *See, e.g.*, *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982) ("The language of section 1806(f) clearly anticipates that an *ex parte*, *in camera* determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring *only* when necessary") (emphasis in original); *United States v. Dhirane*, 896 F.3d 295, 300 (4th Cir. 2018); *United States v. Omar*, 786 F.3d 1104, 1111 (8th Cir. 2015) (citing *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991)); *El-Mezain*, 664 F.3d at 566-67; *United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010); *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984). As the court stated in *United States v. Daoud*, "[u]nless and until a district judge performs his or her statutory duty of attempting to determine the legality of the surveillance without revealing any of the fruits of the surveillance to defense

---

[15] **[CLASSIFIED INFORMATION REDACTED]**

counsel, there is no basis for concluding that disclosure is necessary in order to avert an erroneous conviction." 755 F.3d 479, 484 (7th Cir. 2014).

If the district court can accurately determine the legality of the electronic surveillance and physical search based on its *in camera, ex parte* review, then the court may not order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. *See Squillacote*, 221 F.3d at 554; *Dhirane,* 896 F.3d at 300-01*; El-Mezain*, 664 F.3d at 566*; Abu-Jihaad,* 630 F.3d at 129; *Rosen,* 447 F. Supp. 2d at 546.

1. *In Camera, Ex Parte* Review is the Rule

Federal circuit courts, including the Fourth Circuit, have ruled that FISA anticipates that an *in camera, ex parte* determination is "the rule," while disclosure and an adversary hearing are the exception occurring only when necessary. *Squillacote*, 221 F.3d at 554 (quoting *Belfield*, 692 F.2d at 147); *United States v. Hassan*, 742 F.3d 104, 138 (4th Cir. 2014) ("We have emphasized that, where the documents 'submitted by the government [are] sufficient' to 'determine the legality of the surveillance,' the FISA materials should not be disclosed") (quoting *Squillacote*, 221 F.3d at 554); *Rosen*, 447 F. Supp. 2d at 546; *Omar*, 786 F.3d at 1110 (quoting *Isa*, 923 F.2d at 1306); *El-Mezain*, 664 F.3d at 567 ("[D]isclosure of FISA materials is the exception and *ex parte*, *in camera* determination is the rule") (citing *Abu Jihaad*, 630 F.3d at 129); *Daoud*, 755 F.3d at 481 (The district judge "must, in a non-public ('*in camera*'), nonadversarial ('*ex parte*') proceeding, attempt to determine whether the surveillance was proper"); *Duggan*, 743 F.2d at 78.[16]

[16] In *Duggan*, the Second Circuit explained that disclosure might be necessary "if the judge's initial review revealed potential irregularities such as 'possible misrepresentations of fact, vague identification of persons to be surveilled or surveillance records which include[] a significant amount of nonforeign intelligence information, calling into question compliance with

In fact, every district court but one (whose decision was overturned)[17] that has addressed a motion to disclose FISA materials or to suppress FISA information has been able to decide the legality of the FISA collection at issue based on its *in camera, ex parte* review.[18] And every appellate court to have reviewed such a determination has affirmed.[19]

The exhibits in the Sealed Appendix confirm that there is nothing extraordinary about the instant FISA-authorized electronic surveillance and physical search that would justify the production and disclosure of highly sensitive and classified FISA materials or the suppression of FISA-obtained or -derived evidence. The FISA materials are well-organized and easily

---

the minimization standards contained in the order.'" 743 F.2d at 78 (quoting S. Rep. No. 95-604, pt. 1, 95th Cong., 1st Sess., at 58 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3960).

[17] The district court in *United States v. Daoud*, No. 12 cr 723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014), ruled that it could make the required determination, but still ordered disclosure of the FISA materials. The Government appealed the *Daoud* court's order to the Seventh Circuit, which overturned the district court's decision to disclose, stating, "So clear is it that the materials were properly with-held from defense counsel that there is no need for a remand to enable the district judge to come to the same conclusion, because she would have to do so." *Daoud*, 755 F.3d at 485.

[18] *See, e.g.*, *United States v. Kokayi*, 1:180cr-410 (LMB), 2019 WL 1186846, at *5-6 (E.D. Va. Mar. 13, 2019); *Rosen*, 447 F. Supp. 2d at 546; *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. May 17, 2006); *United States v. Nicholson*, 955 F. Supp. 588, 592 & n.11 (E.D. Va. 1997); *United States v. Ramic*, No. 1:21-CR-00013-GNS-HBB, 2024 WL 1494755, at *3-4 (W.D. Ky. Apr. 5, 2024); *United States v. Al-Safoo*, 18-CR-696, 2021 WL 1750313, at *3-4 (N.D. Ill. May 4, 2021); *United States v. Chi Ping Ho*, 17 Cr. 779 (LAP), 2018 WL 5777025, at *5 (S.D.N.Y. Nov. 2, 2018); *United States v. Medunjanin*, No. 10 CR 19 1 (RJD), 2012 WL 526428, at *9 (E.D.N.Y. Feb. 16, 2012); *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310-11 (D. Conn. 2008), *aff'd*, 630 F.3d 102 (2d Cir. 2010); *United States v. Warsame*, 547 F. Supp. 2d 982, 987-89 (D. Minn. 2008); *United States v. Sattar*, No. 02 CR. 395 JGK, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003); *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. 1990); *United States v. Falvey*, 540 F. Supp. 1306, 1315-16 (E.D.N.Y. 1982).

[19] *See, e.g.*, *Belfield*, 692 F.2d at 147; *Squillacote*, 221 F.3d at 554; *Hassan*, 742 F.3d at 138-39; *Omar*, 786 F.3d at 1110-11; *El-Mezain*, 664 F.3d at 565-67; *United States v. Damrah*, 412 F.3d 618, 624-25 (6th Cir. 2005); *Isa*, 923 F.2d at 1306; *Ott*, 827 F.2d at 476; *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987).

reviewable by the Court *in camera* and *ex parte*, and they are fully and facially sufficient to allow the Court to make an accurate determination that the FISA information was lawfully acquired and that the electronic surveillance and physical search were made in conformity with an order of authorization or approval. In other words, the materials presented "are straightforward and readily understood." *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986). Moreover, as in other cases, determining the legality of the FISA collection is not complex. *See Belfield*, 692 F.2d at 147; *Abu-Jihaad*, 531 F. Supp. 2d at 310 ("Court review of the FISA materials in this case is relatively straightforward and not complex"); *Warsame*, 547 F. Supp. 2d at 987 (finding that the "issues presented by the FISA applications are straightforward and uncontroversial"); *Thomson*, 752 F. Supp. at 79. This Court, much like the aforementioned courts, can review the FISA materials *in camera* and *ex parte* and make the requisite legal determination without an adversarial hearing.

In addition to the specific harm caused by disclosing the FISA materials, which is detailed in the classified declaration of a high-ranking FBI official in support of the Declaration and Claim of Privilege of the AAG/NS, the rationale for non-disclosure is clear: "Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to *anyone* not involved in the surveillance operation in question, whether or not she happens for unrelated reasons to enjoy security clearance." *Ott*, 827 F.2d at 477 (emphasis in original); *accord United States v. Amawi*, 531 F. Supp. 2d 832, 838 (N.D. Ohio 2008) (finding that the FISA materials contained considerable "operational and technical information" the disclosure of which could adversely affect the Government's ability to obtain "useful foreign intelligence information"), *aff'd*, 695 F.3d 457 (6th Cir. 2012); *Isa*, 923 F.2d at 1306 (the court's "study of the materials leaves no

doubt that substantial national security interests required the *in camera, ex parte* review, and that the district court properly conducted such a review"); *Medunjanin*, 2012 WL 526428, at *9 (finding persuasive the Government's argument that "unsealing the FISA materials in this case would provide the defense with unnecessary details of an extraordinarily sensitive anti-terrorism investigation").

Confidentiality is critical to national security. "If potentially valuable intelligence sources" believe that the United States "will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information to [the U.S. Government] in the first place." *CIA v. Sims*, 471 U.S. 159, 175 (1985); *see also Phillippi v. CIA*, 655 F.2d 1325, 1332-33 (D.C. Cir. 1981). When considering whether disclosing classified sources, methods, techniques, or information would harm national security, federal courts have expressed great reluctance to replace the considered judgment of Executive Branch officials who must weigh complex factors in determining whether disclosing information may lead to an unacceptable risk of compromising the intelligence-gathering process, and who must determine whether foreign agents, spies, and terrorists can assemble a mosaic of information that, when revealed, could harm U.S. national security. *See Sims*, 471 U.S. at 180; *Amawi*, 531 F. Supp. 2d at 837 (refusing to "second-guess" the Attorney General's declaration stating that disclosure or an adversary hearing would harm national security); *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods"); *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) ("each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other

bits of information even when the individual piece is not of obvious importance in itself"). An adversarial hearing is not only unnecessary to aid the Court in the task before it, but would create potential dangers that courts have consistently sought to avoid.

As the *Belfield* court explained:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law enforcement surveillance.

692 F.2d at 148 (footnotes and citations omitted); *see also United States v. Stewart*, 590 F.3d 93, 128 (2d Cir. 2009) ("FISA applications are likely to contain allegedly sensitive information relating to perceived issues of national security. . . . For[] this reason, '*ex parte*, *in camera* determination is to be the rule.'") (quoting *Duggan*, 743 F.2d at 78); *Daoud*, 755 F.3d at 483 ("Everyone recognizes that privacy is a legally protectable interest, and it is not an interest of private individuals alone. [FISA] is an attempt to strike a balance between the interest in full openness of legal proceedings and the interest in national security, which requires a degree of secrecy concerning the government's efforts to protect the nation."); *ACLU Found. of So. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) (citing *Belfield* for the proposition that Section 1806(f) "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance").

2. *In Camera, Ex Parte* Review is Constitutional

Every federal court that has considered the matter—including in the Eastern District of Virginia—has affirmed that FISA's *in camera, ex parte* review provisions are constitutional.[20]

In sum, FISA mandates a process by which the district court must conduct an initial *in camera, ex parte* review of the FISA materials to determine whether the FISA information was lawfully acquired and whether the relevant electronic surveillance and physical search conformed with an order of authorization or approval. This *in camera, ex parte* review process is the rule in such cases and that procedure is constitutional. In this matter, the AAG/NS filed the required declaration invoking that procedure and has declared that disclosure or an adversary hearing would harm national security. Thus, an *in camera, ex parte* review by this Court is the appropriate venue in which to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search conformed with an order of authorization or approval.

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

In evaluating the legality of the FISA collection, a district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause

---

[20] *See, e.g.*, *Dhirane,* 896 F.3d at 300-01; *Belfield*, 692 F.2d at 147-49; *Damrah*, 412 F.3d at 624; *Isa*, 923 F.2d at 1306-07; *El-Mezain*, 664 F.3d at 567-68; *Abu-Jihaad*, 630 F.3d at 129; *Ott*, 827 F.2d at 476-77; *ACLU Foundation*, 952 F.2d at 465; *Benkahla,* 437 F. Supp. 2d at 554; *United States v. Nicholson*, No. 09-CR-40-BR, 2010 WL 1641167, at *3-4 (D. Or. Apr. 21, 2010); *United States v. Jayyousi*, No. 04-60001, 2007 WL 851278, at *7-8 (S.D. Fla. Mar. 15, 2007); *United States v. Spanjol*, 720 F. Supp. 55, 59 (E.D. Pa. Aug. 22, 1989), *aff'd*, 958 F.2d 365 (3d Cir. 1992); *United States v. Megahey*, 553 F. Supp. 1180, 1194 (E.D.N.Y. Dec. 1, 1982); *Falvey*, 540 F. Supp. at 1315-16.

showing required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31; *see also* 50 U.S.C. §§ 1806(f), 1825(g).

1. Standard of Review of Probable Cause

Although federal courts have not resolved whether the FISC's probable cause determination should be reviewed *de novo* or accorded due deference, the material under review here satisfies either standard of review. *See Omar*, 786 F.3d at 1112 ("[W]e have no hesitation concluding that probable cause under FISA existed under any standard of review."); *Abu-Jihaad*, 630 F.3d at 130 ("Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submissions in this case would easily allow it to clear a higher standard of review"). The Fourth Circuit and the Eastern District of Virginia are among the courts that have reviewed the FISC's probable cause determination *de novo*. *See Hassan*, 742 F.3d at 138-39 (noting that the district court correctly reviewed the FISA materials *de novo* and "with a presumption of validity accorded to the certifications"); *Squillacote*, 221 F.3d at 554; *Rosen*, 447 F. Supp. 2d at 545.

2. Probable Cause Standard

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance or physical search is directed is, or is about to be, used, owned, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1805(a), 1824(a); *Abu-Jihaad*, 630 F.3d at 130. It is this standard—not the standard applicable to criminal search warrants—that this Court must apply. *Omar*, 786 F.3d at 1111 ("[R]ather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power.") (quoting *El-Mezain*, 664 F.3d at 564);

United States v. Cavanagh, 807 F.2d. 787, 790 (9th Cir. 1987) (citing *United States v. United States District Court ("Keith")*, 407 U.S. 297, 322 (1972)).

The probable cause threshold that the Government must satisfy before receiving authorization to conduct electronic surveillance or a physical search under FISA complies with the Fourth Amendment's reasonableness standard. Federal courts have uniformly rejected the argument that FISA's different probable cause standard violates the Fourth Amendment's reasonableness requirement. *See, e.g.*, *Abu-Jihaad*, 630 F.3d at 120 (listing sixteen cases that ruled FISA does not violate the Fourth Amendment).

Although the probable cause findings required under FISA differ from the findings applicable to criminal search warrants, the FISA standard is no less constitutional. The Supreme Court has stated that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens." *Keith*, 407 U.S. at 322-23 (recognizing that domestic security surveillance "may involve different policy and practical considerations from the surveillance of 'ordinary crime'"). In *Keith*, the Supreme Court acknowledged that: (1) the "focus of . . . surveillance [in domestic security investigations] may be less precise than that directed against more conventional types of crime"; (2) unlike ordinary criminal investigations, "[t]he gathering of security intelligence is often long range and involves the interrelation of various sources and types of information"; and (3) the "exact targets of such surveillance may be more difficult to identify" than in surveillance operations of ordinary crimes under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510-2522) (Title III). *Id.* Although *Keith* was decided before FISA's enactment and addressed purely domestic security surveillance, the rationale underlying *Keith*

applies *a fortiori* to foreign intelligence surveillance, where the Government's interest, at least from a national security perspective, would typically be more pronounced.

FISA was enacted partly in response to *Keith*. In constructing FISA's framework, Congress addressed *Keith*'s question of whether departures from traditional Fourth Amendment procedures "are reasonable, both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens," and "concluded that such departures are reasonable." *See* S. Rep. No. 95-701, at 11-12, 1978 U.S.C.C.A.N. at 3980.

Similarly, many courts—including the Fourth Circuit and the FISC of Review—have relied on *Keith* in holding that FISA collection conducted pursuant to a FISC order is reasonable under the Fourth Amendment. *See Pelton*, 835 F.2d at 1075 (denying a defendant's claim that FISA's procedures violate the Fourth Amendment); *In re Sealed Case*, 310 F.3d 717, 738, 746 (FISA Ct. Rev. 2002) (finding that while many of FISA's requirements differ from those in Title III, few of those differences have constitutional relevance); *see also Duggan*, 743 F.2d at 74 (holding that FISA does not violate the Fourth Amendment); *United States v. Ning Wen*, 477 F.3d 896, 898 (7th Cir. 2007) (holding that FISA is constitutional despite using "a definition of 'probable cause' that does not depend on whether a domestic crime has been committed"); *Cavanagh*, 807 F.2d at 790-91 (holding that FISA satisfies the Fourth Amendment requirements of probable cause and particularity).

[CLASSIFIED INFORMATION REDACTED]

3. Standard of Review of Certifications

Under FISA, "[t]he FISA Judge need only determine that the application contains all of the statements and certifications required by the Act if the target is a non-United States person, whereas [the FISA Judge] must also find that the certifications are not 'clearly erroneous' if the

target is a United States person." *Duggan*, 743 F.2d at 75; *United States v. Campa*, 529 F.3d 980, 994 (11th Cir. 2008). A finding is "clearly erroneous" when "although there is evidence to support it, the reviewing court on the [basis of the] entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); *United States v. Pulley*, 987 F.3d 370, 376 (4th Cir. 2021).

When a FISA application is presented to the FISC, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77. Likewise, Congress intended that the reviewing district court should "have no greater authority to second-guess the executive branch's certifications than has the FISA judge." *Id.* Certifications submitted in support of a FISA application should be "subjected only to minimal scrutiny by the courts," *Badia*, 827 F.2d at 1463, and are "presumed valid." *See Hassan*, 742 F.3d at 138-39 (stating that the district court correctly reviewed the materials with "a presumption of validity accorded to the certifications"); *Pelton*, 835 F.2d at 1076 (where "the statutory application was properly made and earlier approved by a FISA judge, it carries a strong presumption of veracity and regularity in a reviewing court"); *see also Rosen*, 447 F. Supp. 2d at 545 ("the certifications contained in the applications should be 'presumed valid'"); *Campa*, 529 F.3d at 993.

4. FISA is Subject to the "Good-Faith" Exception

Even assuming *arguendo* that this Court determines that a FISC order was not supported by probable cause, or that the FISA certification requirements were not met, the evidence obtained or derived from the FISA-authorized electronic surveillance and physical search is still admissible under the "good faith" exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984). Numerous courts have stated that the good faith exception applies

to FISA evidence. For instance, in *Ning Wen*, the Seventh Circuit, relying on *Leon*, stated that federal officers can rely in good faith on a FISA warrant. 477 F.3d at 897. In so doing, the *Ning Wen* court noted:

> [T]he exclusionary rule must not be applied to evidence seized on the authority of a warrant, even if the warrant turns out to be defective, unless the affidavit supporting the warrant was false or misleading, or probable cause was so transparently missing that 'no reasonably trained officer [would] rely on the warrant.'

Id. (quoting *Leon*, 468 U.S. at 923); *see also United States v. Mubayyid*, 521 F. Supp. 2d 125, 140 n.12 (D. Mass. 2007) (noting that even if the FISA "statute were deemed unconstitutional," the exclusionary rule would not apply to evidence obtained pursuant to FISA-authorized surveillance under *Leon* because "the government proceeded in good faith and in reasonable reliance on the FISA orders"); *United States v. Ahmed*, 1:06-cr-147-WSD-GGB, 2009 U.S. Dist. LEXIS 120007, at *25 n.8 (N.D. Ga. Mar. 19, 2009) ("[t]he FISA evidence obtained . . . would be admissible under *Leon*'s 'good faith' exception to the exclusionary rule were it not otherwise admissible under a valid warrant"); *United States v. Marzook*, 435 F. Supp. 2d 778, 790-91 (N.D. Ill. 2006) (holding, in an analogous context, that "the FBI's reliance on the Attorney General's approval under Executive Order No. 12333 – an order that no court has found unconstitutional – was [] objectively reasonable because that order pertains to foreign intelligence gathering").

Here, there is no basis to find that the FISC was misled by any declaration(s) or certification(s) at issue, as these documents were neither deliberately nor recklessly false. *See Leon*, 468 U.S. at 914-15. Further, there is no indication that the FISC abandoned its judicial role or somehow failed to act in a neutral and detached manner when authorizing the electronic surveillance and physical search at issue. *See id.* Moreover, as the Court will see from its *in camera*, *ex parte* review of the FISA materials, facts establishing the requisite probable cause

were submitted to the FISC, the FISC's order(s) contained all the requisite findings, and well-trained officers reasonably relied on those order(s). Thus, even if the Court questions whether sufficient probable cause supported a FISC order, the information obtained pursuant to that order would be admissible under *Leon*'s good faith exception.

Lastly, consistent with its underlying rationale, a court should not impose the exclusionary rule to punish an officer who acts in objectively reasonable reliance on a duly-issued warrant or enacted statute. In *Illinois v. Krull*, the Supreme Court "ruled categorically that 'suppressing evidence obtained by an officer acting in objectively reasonable reliance on a statute' would not further the purposes of the exclusionary rule, even if that statute is later declared unconstitutional." *Duka*, 671 F.3d at 346 (quoting *Krull*, 480 U.S. 340, 349-50 (1987)). The same is true for warrants that are later determined to be invalid. *See United States v. Helton,* 35 F.4th 511, 521 (6th Cir. 2022) (quoting *Leon* for the proposition "that if 'the evidence was obtained in objectively reasonable reliance on the subsequently invalidated search warrant, however, it should not be suppressed"). "Because the rule 'is designed to deter police misconduct,' it applies only where it will 'alter the behavior of individual law enforcement officers or the policies of their departments.'" *Duka*, 671 F.3d at 346 (quoting *Leon*, 468 U.S. at 916-18). Here, the exclusion of FISA information would serve no such deterrent purpose. *See Davis v. United States*, 564 U.S. 229, 237 (2011); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 282-84 (S.D.N.Y. 2000).

IV. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH AT ISSUE WERE LAWFULLY AUTHORIZED AND CONDUCTED

This section first discusses the materials in the Sealed Appendix to demonstrate, considering the standards of review described above, that the FISA authorities in this matter were lawfully *authorized.* Then this section addresses the Government's good faith compliance

with proper minimization procedures and related requirements to demonstrate that the electronic surveillance and physical search at issue were lawfully *conducted*.

A. THE INSTANT FISA APPLICATION(S) MET FISA'S PROBABLE CAUSE STANDARD

[CLASSIFIED INFORMATION REDACTED]

1. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

2. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

a. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

b. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

c. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

d. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

e. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

f. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

g. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

3. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

a. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

b. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

c. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

d. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

e. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

f. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

g. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

h. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

i. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

j. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

k. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

l. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

m. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

B. THE CERTIFICATION(S) COMPLIED WITH FISA

[CLASSIFIED INFORMATION REDACTED]

1. Foreign Intelligence Information

[CLASSIFIED INFORMATION REDACTED]

2. "A Significant Purpose"

[CLASSIFIED INFORMATION REDACTED]

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED INFORMATION REDACTED]

C. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED INFORMATION REDACTED]

1. The Standard Minimization Procedures

Once a reviewing court is satisfied that the FISA information was lawfully acquired, it must then examine whether the relevant electronic surveillance and physical search were lawfully conducted. *See* 50 U.S.C. §§ 1806(e)(2), 1825(g). To do so, the reviewing court must determine whether the Government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

[CLASSIFIED INFORMATION REDACTED]

FISA's legislative history and relevant case law show that the definitions of "minimization procedures" and "foreign intelligence information" were intended to consider the realities of collecting foreign intelligence because the activities of persons engaged in clandestine intelligence gathering or international terrorism are often not obvious. *See Rahman*, 861 F. Supp. at 252-53. The degree to which information must be minimized varies in each investigation, such that less minimization at acquisition is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d at 741; *see also Bin Laden*, 126 F. Supp. 2d at 286 ("more extensive monitoring and greater leeway in minimization efforts are permitted in a case like this given the world-wide, covert and diffuse nature of the international terrorist group(s) targeted" [internal quotation marks omitted]).

Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities, and other practices designed to conceal the breadth and aim of their operations, organization, activities, and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center referred to the bomb plot as the "study" and to terrorist materials as "university papers").

As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *Kevork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., pt. 1, at 55 (1978)); *see also United States v. Hammoud*, 381 F.3d 316, 334 (4th Cir. 2004) (citing *Salameh*, 152 F.3d at 154), *vacated on other grounds*, 543 U.S.

1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005); *In re Sealed Case*, 310 F.3d at 740-41; *Thomson*, 752 F. Supp. at 81 (noting that it is permissible to retain and disseminate "bits and pieces" of information until the information's "full significance becomes apparent") (citing H.R. Rep. No. 95-1283, pt. 1, at 58); *Bin Laden*, 126 F. Supp. 2d at 286. Likewise, "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." *Rahman*, 861 F. Supp. at 252-53 (citing H.R. Rep. No. 95-1283, pt. 1, at 55, 59). The Government must also be given flexibility where the conversations are carried out in a foreign language. *Mubayyid*, 521 F. Supp. 2d at 134; *Rahman*, 861 F. Supp. at 252. As a result, "courts have construed 'foreign intelligence information' broadly and sensibly [and] allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a U.S. person who is acting as an agent of a foreign power. As Congress explained:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

H.R. Rep. No. 95-1283, pt. 1, at 58. Indeed, at least one court has cautioned that, when a U.S. person communicates with an agent of a foreign power, the Government would be "remiss in

meeting its foreign counterintelligence responsibilities if it did not investigate such contacts and gather information to determine the nature of those activities." *Thomson*, 752 F. Supp. at 82.

Considering these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. Rep. No. 95-701, at 39, 1978 U.S.C.C.A.N. at 3973, 4008 (quoting *United States v. Bynum,* 485 F.2d 490, 500 (2d Cir. 1973)). The Fourth Circuit reached the same conclusion in *Hammoud*, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance." 381 F.3d at 334.

Accordingly, in reviewing minimization efforts, the test is neither whether innocent conversations were intercepted, nor whether mistakes were made for certain communications. Rather, as the Supreme Court stated in the context of Title III surveillance, there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." *Scott v. United States*, 436 U.S. 128, 136-37 (1978). Absent a charge the minimization procedures were disregarded completely, the test of compliance is whether a good-faith effort to minimize was attempted. *Rosen*, 447 F. Supp. 2d at 551; *see also Hammoud*, 381 F.3d at 334 ("[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information"); S. Rep. No. 95-701, at 39-40, 1978 U.S.C.C.A.N. at 4008-09 (stating that the court's role is to decide whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion").

Moreover, even if it is not foreign intelligence information, FISA does not require the Government to minimize information that is "evidence of a crime." 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); *see also Isa*, 923 F.2d at 1304 (noting that "[t]here is no requirement that the 'crime'

be related to foreign intelligence"). Thus, if a U.S. person's communications may be evidence of a crime or establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See Isa*, 923 F.2d at 1305.

Even if certain communications were not properly minimized in accordance with the SMPs, suppression would be inappropriate for those other communications that met the standard. *Cf. United States v. Falcone*, 364 F. Supp. 877, 886-87 (D. N.J. 1973), *aff'd*, 500 F.2d 1401 (3d Cir. 1974) (Title III). Absent evidence that there has been a "complete" disregard for the minimization procedures, the fact that some communications should have been minimized does not affect the admissibility of others that were properly acquired and retained. FISA's legislative history reflects that Congress intended only a limited sanction for minimization errors:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

H.R. Rep. No. 95-1283, pt. 1, at 93; *see also Falcone*, 364 F. Supp. at 886-87; *Medunjanin*, 2012 WL 526428, at *12 (disclosure and suppression not warranted where "failure to adhere to [the minimization] protocol was *de minimis*").

2. The FISA Information Was Appropriately Minimized

[CLASSIFIED INFORMATION REDACTED]

Based on this information, the Government lawfully conducted the FISA collection discussed herein, and this Court should find that the FISA collection was lawfully conducted under the minimization procedures approved by the FISC and applicable to the FISA collection.

V. THE COURT SHOULD REJECT CHHIPA'S LEGAL ARGUMENTS

Chhipa asks this Court to (1) suppress all the FISA-obtained or -derived evidence; (2) suppress all material and any fruits thereof collected under Section 702; and (3) disclose the underlying applications for FISA warrants, Section 702 material, querying information, and all information on other government surveillance programs used to collect his information. Mot. at 1. For the reasons set forth below, his arguments are without merit.

A. Chhipa Has Not Established Any Basis to Suppress the FISA Information

In support of his request to suppress the FISA information, Chhipa argues that the FISA applications may have: (1) failed to establish probable cause; (2) relied on raw intelligence; (3) relied on illegitimate and/or illegal sources of information; (4) relied on First Amendment-protected activity; (5) contained intentional or reckless falsehoods or omissions; (6) omitted the required certifications, including that a significant purpose of the FISA surveillance was the collection of foreign intelligence information; and (7) not contained or implemented the requisite minimization procedures. *See* Mot. at 7-25. This Court should reject each of these arguments for the reasons discussed below.

1. The Government Satisfied the Probable Cause Standard

[CLASSIFIED INFORMATION REDACTED]

Both the Fourth Circuit and judges in this district have consistently denied challenges to the FISC's probable cause determinations. *See, e.g., Hassan*, 742 F.3d at 139; *Hammoud*, 381 F.3d at 332-33; *Squillacote*, 221 F.3d at 554; *Pelton*, 835 F.2d at 1075-76; *Rosen*, 447 F. Supp. 2d at 550; *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. June 22, 2011); *Kokayi*, 2019 WL 1186846, at *4; *United States v. Elshinawy*, No. CR ELH-16-0009, 2017 WL 1048210, at *10 (D. Md. Mar. 20, 2017). As discussed in this brief, FISA requires a finding of probable

cause to believe that the target of the electronic surveillance or physical search is a foreign power or the agent or a foreign power. *See* 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). "Probable cause means more than bare suspicion but less than absolute certainty[,]" and in making the probable cause determination, FISA permits a judge to "consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." *Rosen*, 447 F. Supp. 2d at 549 (quoting *Mason v. Godinez*, 47 F.3d 852, 855 (7th Cir. 1995) and 50 U.S.C. § 1805(b)). The FISA probable cause standard "does not necessarily require a showing of an imminent violation of criminal law" because Congress intended a different showing of probable cause than that applicable to ordinary cases. *Id.* at 549 (quoting *In re Sealed Case*, 310 F.3d at 738).

[CLASSIFIED INFORMATION REDACTED]

2. Raw Intelligence is Not Inherently Unreliable

Next, Chhipa speculates that the FISA applications at issue contained "raw intelligence." Mot. at 10-11. Chhipa does not define "raw intelligence," and cites no authority supporting his position. Regardless, the D.C. Circuit found no basis for "a per se rule that information contained in an intelligence report is inherently unreliable." *Barhoumi v. Obama*, 609 F.3d 416, 429 (D.C. Cir. 2010). To the contrary, such information need only "be presented in a form, or with sufficient additional information, that permits . . . [the] court to assess its reliability." *Id.* (quoting *Parhat v. Gates*, 532 F.3d 834, 849 (D.C. Cir. 2008) ("[W]e do not suggest that hearsay evidence is never reliable")).

The same is true in the context of criminal search warrants. In making probable cause determinations based on the totality of the circumstances, courts routinely review information presented in search warrant affidavits for indicia of reliability or independent corroboration. *See*

Illinois v. Gates, 462 U.S. 213, 238 (1983) (probable cause sufficient, based on totality of the circumstances, where anonymous informant's recitation of detailed facts was corroborated by police observation); *Draper v. United States*, 358 U.S. 307, 313 (1959) (probable cause sufficient where hearsay information from previously reliable source was corroborated by independent police investigation); *United States v. Martinez-Garcia*, 397 F.3d 1205, 1216-17 (9th Cir. 2005) (probable cause sufficient where reliable informant told police he had purchased drugs from defendant, and police observed three controlled drug buys). As the case law above counsels, this Court should decline to suppress the FISA information even if "raw intelligence" was presented to the FISC.

[CLASSIFIED INFORMATION REDACTED]

3. The FISA Application(s) Was/Were Based on Lawfully Obtained Information

[CLASSIFIED INFORMATION REDACTED]

4. The FISA Application(s) Was/Were Not Based Solely on First Amendment-Protected Activities

[CLASSIFIED INFORMATION REDACTED]

5. *Franks v. Delaware* Does Not Require Suppression of the FISA Information or Disclosure of the FISA Materials

Chhipa next claims that the FISA application(s) may contain intentional or reckless falsehoods or omissions, in contravention of *Franks v. Delaware*, 438 U.S. 154 (1978), and demands a *Franks* hearing and disclosure of the FISA materials, along with suppression of the FISA information. Mot. at 16-20. But as the Court's review of the FISA materials will show, no material false statements or omissions exist regarding the FISA information. Thus, this Court should deny Chhipa's suppression motion, and decline his request to order the disclosure of the FISA materials so that he can pursue a *Franks* hearing.

To merit a *Franks* hearing, a defendant must make a "substantial preliminary showing" that the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit, and that the resulting misrepresentation was necessary to the finding of probable cause. *See Franks*, 438 U.S. at 155-56. Courts apply the same standard when a defendant seeks a *Franks* hearing as part of a challenge to FISA collection: to obtain a hearing, a defendant must "make 'a substantial preliminary showing that a false statement knowingly or intentionally, or with reckless disregard for the truth, was included' in the application and that the allegedly false statement was 'necessary' to the FISA Judge's approval of the application." *Duggan*, 743 F.2d at 77 n.6 (quoting *Franks*, 438 U.S. at 155-56). Only after a defendant makes the requisite showing may the Court conduct a *Franks* hearing to determine if there are material misrepresentations of fact, or omissions of material fact, in the FISA applications sufficient to warrant suppression of the FISA-obtained or -derived evidence.[21] *See Franks*, 438 U.S. at 171.

[CLASSIFIED INFORMATION REDACTED]

Additionally, this Court should decline Chhipa's request to order the disclosure of the FISA materials so he can pursue a *Franks* hearing. Mot. at 20. This approach would allow him, and defendants in every case, to obtain the FISA materials merely by alleging some theoretical impropriety. Disclosing FISA materials to defendants would then become the rule, violating Congress' clear intention, set forth in 50 U.S.C. §§ 1806(f) and 1825(g), that the FISA materials be reviewed *in camera* and *ex parte* consistent with the realities of modern intelligence needs

[21] Indeed, even if a defendant offers sufficient proof to show that an affidavit involved false statements or omissions, a hearing should not be held where the affidavit would still provide probable cause if the allegedly false material were eliminated, or if the allegedly omitted information were included. *Franks*, 438 U.S. at 171; *United States v. Colkley,* 899 F.2d 297, 300 (4th Cir. 1990); *United States v. Ketzeback*, 358 F.3d 987, 990 (8th Cir. 2004); *United States v. Martin*, 615 F.2d 318, 328 (5th Cir. 1980).

and investigative techniques. Courts have acknowledged that FISA does not allow for such disclosure without establishing a basis for it. For instance, the *Daoud* court noted that it was "hard" for a defendant to make the *Franks* showing "without access to the classified [FISA] materials," but the "drafters of [FISA] devised a solution: the judge makes the initial determination, based on full access to all classified materials . . . ." 755 F.3d at 483-84. Similarly, in *Belfield*, the court noted that "Congress was also aware of these difficulties [faced by defense counsel without access to FISA materials and] chose to resolve them through means other than mandatory disclosure." 692 F.2d at 148.

Courts have rejected other defendants' attempts to force a *Franks* hearing by speculating about the contents of FISA applications, and this Court should do so here. *See United States v. Aziz*, 228 F. Supp. 3d 363, 371 (M.D. Pa. 2017) (finding defendant's suggestion of "the 'possibility' of error" provided no arguable basis to convene a *Franks* hearing); *United States v. Huang*, 15 F. Supp. 3d 1131, 1142 (D.N.M. 2014) ("Defendant has not offered anything more than conclusory speculations about allegations of falsehoods in the FISA affidavit"); *United States v. Hussein*, 13-CR-1514-JM, 2014 WL 1682845, at *5 (S.D. Cal. Apr. 29, 2014) (rejecting the defendant's unsubstantiated demand for a *Franks* hearing to probe the FISA application); *Abu-Jihaad*, 531 F. Supp. 2d at 311-12; *United States v. Hassoun*, No. 04-CR-60001, 2007 WL 1068127, at *4 (S.D. Fla. Apr. 4, 2007); *United States v. Kashmiri*, No. 09-CR-830, 2010 WL 4705159, at *6 (N.D. Ill. Nov. 10, 2010) (noting that the court "has already undertaken a process akin to a *Franks* hearing through its *ex parte*, *in camera* review"); *Mubayyid*, 521 F. Supp. 2d at 131 ("The balance struck under FISA – which is intended to permit the gathering of foreign intelligence under conditions of strict secrecy, while providing for judicial review and other appropriate safeguards – would be substantially

undermined if criminal defendants were granted a right of disclosure simply to ensure against the possibility of a *Franks* violation.").

Chhipa failed to establish the prerequisites for an adversarial hearing, and his attempt to obtain disclosure of the FISA materials to meet that burden runs counter to FISA, *Franks*, precedent, and Congressional intent. This Court should deny his request for a *Franks* hearing and deny his request for suppression of the FISA information.

6. The Government Satisfied the Applicable "Significant Purpose" Standard and the Certification(s) Complied with FISA

Chhipa also speculates that the collection of foreign intelligence information was not a significant purpose of the FISA surveillance, and that the FISA application(s) may not have included the required certification(s). Mot. at 20-24. Courts have consistently denied such speculative claims, *see, e.g., Hammoud*, 381 F.3d at 333, and this Court should too.

[CLASSIFIED INFORMATION REDACTED]

Despite conceding that the only Circuit decisions on this point are adverse, Chhipa raises a challenge to the constitutionality of the significant purpose standard, arguing it violates the Fourth Amendment. Mot. at 21, n.9. But other than the now-vacated *Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007),[22] which has been legally null for more than 15 years, each court to have considered the PATRIOT Act amendment setting forth the significant purpose test has held that it is constitutional. *See, e.g., Abu-Jihaad*, 630 F.3d at 128 ("FISA's 'significant purpose' requirement . . .

[22] *Mayfield*, a civil case, found that FISA's "significant purpose" standard was unconstitutional. 504 F. Supp. 2d at 1042-43. The Ninth Circuit vacated the case because the plaintiff lacked standing. *See Mayfield v. United States*, 599 F.3d 964, 973 (9th Cir. 2010). When a higher court vacates a judgment, as in *Mayfield*, "it deprives the [lower] court's opinion of precedential effect." *Los Angeles County v. Davis*, 440 U.S. 625, 634 n.6 (1979).

is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering . . . [t]he fact that the government may also be pursuing other purposes, including gathering evidence for criminal prosecution, compels no different conclusion"); *Duka*, 671 F.3d at 343; *Damrah*, 412 F.3d at 625; *In re Sealed Case,* 310 F.3d at 746.

In sum, the Court's *in camera*, *ex parte* review of the FISA materials will dispel Chhipa's speculation that the certification(s) were flawed or missing. To the contrary, all the required certification(s) and statements were properly made and included in the application(s), the foreign intelligence interests of the United States were a significant purpose of the electronic surveillance and physical search, and the application(s) sought the type of foreign intelligence information identified. For these same reasons, and considering that the certification(s) are presumed to be valid, this Court should deny Chhipa's suppression motion and decline his request to order disclosure of the FISA application(s) so defense counsel can "provide input" on the certification(s). Mot. at 21.

7. The Government Complied with the Minimization Procedures

Chhipa next claims it "is possible" that the FISA application(s) at issue did not contain adequate minimization procedures, or that the Government did not follow those procedures. Mot. at 24-25. As discussed, FISA requires that the Government comply with all applicable procedures to appropriately minimize information acquired pursuant to FISA. *See* 50 U.S.C. § 1805(a)(3). Both the Fourth Circuit and the Eastern District of Virginia, in addressing minimization, have acknowledged that "courts have construed 'foreign intelligence information' broadly and sensibly [and] allowed the government some latitude in its determination of what is foreign intelligence information," *Rosen*, 447 F. Supp. 2d at 551, as "[i]t is not always immediately clear" whether a particular conversation must be minimized because a "conversation that seems innocuous on one day may later turn out to be of great significance, particularly if the individuals involved are talking in

code." *Hammoud*, 381 F.3d at 334. Indeed, FISA was drafted with the intent to provide "latitude" to the government. *Rosen*, 447 F. Supp. 2d at 552 (citing H.R. Rep. No. 95-1283, pt. 1, at 58).

[CLASSIFIED INFORMATION REDACTED]

B. Chhipa Lacks Standing to Challenge Any Putative Collection under Section 702

[CLASSIFIED INFORMATION REDACTED]

As background, Section 702 authorizes the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. Such surveillance may not intentionally "target a United States person"—whether that person is known to be in the United States or is believed to be outside the United States, 50 U.S.C. § 1881a(b)(1) and (3)—and may not target a person outside the United States "if the purpose . . . is to target a particular, known person reasonably believed to be in the United States," *id.* § 1881a(b)(2). The government's notice obligations regarding the use of FISA information under Section 702 apply if the government (1) "intends to enter into evidence or otherwise use or disclose" (2) "against an aggrieved person" (3) in a "trial, hearing or other proceeding in or before any court, department officer, agency, regulatory body, or other authority of the United States" (4) any "information obtained or derived from" (5) "electronic surveillance of that aggrieved person." 50 U.S.C. §§ 1806(f), 1881e(a) (providing that information acquired pursuant to Sections 702 and 703 of FISA "shall be deemed to be information acquired from electronic surveillance pursuant to" Title I of FISA). When all five criteria are met, the government must provide notice that it intends to use or disclose Section 702 information. An "aggrieved person" is a person who is either the target of an electronic surveillance or one whose communications or activities were subject to electronic surveillance. *Id.* §§ 1801(k), 1881e(a).

Only an aggrieved person may move to suppress evidence obtained or derived from electronic surveillance to which he is an aggrieved person. *Id.* § 1806(e).

[CLASSIFIED INFORMATION REDACTED]

C. Chhipa Has Not Established Any Basis for Disclosing the FISA Materials

Next, Chhipa moves for disclosure of the FISA materials, putative Section 702 material including querying information, and all information on other alleged government surveillance programs, arguing for disclosure under: (1) 50 U.S.C. § 1806(f); (2) 50 U.S.C. § 1806(g) and due process; (3) 18 U.S.C. § 3504 and the Federal Rules of Criminal Procedure; and (4) the adversary system of justice. *See generally* Mot. at 70-78, 81-89. For the following reasons, this Court should deny his request.

1. Disclosure is Not "Necessary" under FISA Section 1806(f)

Chhipa argues for disclosure of the FISA materials under 50 U.S.C. § 1806(f) to provide input on the legality of the surveillance and searches, to address questions regarding probable cause, and to assess whether Section 702 procedures were followed. *See* Mot. at 70-89. But this Court may only disclose the FISA materials when "such disclosure is *necessary* to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f) (emphasis added). Thus, there is only one lawful reason to disclose the FISA materials to defense counsel: that after its review of those materials *in camera* and *ex parte*, this Court cannot determine the legality of the electronic surveillance, physical search, or both, without defense counsel's assistance. 50 U.S.C. §§ 1806(f), 1825(g) (emphasis added); *Daoud*, 755 F.3d at 482; *Duggan*, 743 F.2d at 78. This holding is supported by the legislative history of 50 U.S.C. § 1806(f), which states: "The court may order disclos[ure] to [the defense] . . . only if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance . . .

Once a judicial determination is made that the surveillance was lawful, a motion for discovery . . . must be denied unless disclosure or discovery is required by due process." S. Rep. No. 95-701, at 64-65, 1978 U.S.C.C.A.N., at 4034; *see also Hassan*, 742 F.3d at 138 (where the court "emphasized that, where the documents 'submitted by the government [are] sufficient' to 'determine the legality of the surveillance,' the FISA materials should not be disclosed") (quoting *Squillacote*, 221 F.3d at 454).

Here, Chhipa failed to meet his burden of establishing that this Court cannot determine the legality of the FISA collection without defense counsel's assistance. Although Chhipa purports to flag issues where counsel's input would be "necessary," he failed to explain why this Court cannot address those legal issues just like every other district court has done. As this Court will see from its review, the FISA materials are presented in a well-organized and straightforward manner that allows the Court to determine the lawfulness of the FISA collection without input from Chhipa's counsel.[23]

---

[23] Chhipa's defense counsel notes that she holds a security clearance. Mot. at 72. The only statutory authorities that grant a court discretion to disclose the FISA materials are set out at 50 U.S.C. §§ 1806(f) and 1825(g), and these provisions permit disclosure only where the court finds that it is unable to determine the legality of the electronic surveillance and physical search based on its *in camera, ex parte* review alone and without the assistance of defense counsel. Defense counsel's security clearance does not affect the need to have an *ex parte, in camera* review to determine whether disclosure would harm national security. *See Daoud*, 755 F.3d at 484-86; *see also Medunjanin*, 2012 WL 526428, at *9 ("Defense counsel's security clearances add little to the case for disclosure."). While holding a valid security clearance is a prerequisite to reviewing classified information, it is not a sufficient basis for a court to order disclosure of classified information to defense counsel. Counsel may access classified information only if they hold both the required clearance and a "need-to-know" the information. *Daoud*, 755 F.3d at 484. Cleared counsel only has a "need to know" if the court determining the legality of the surveillance concludes that disclosure is "necessary." *Id.*; *accord Rosen*, 447 F. Supp. 2d at 546. If this Court concludes from its *in camera, ex parte* review of the FISA materials that it can accurately determine the legality of the FISA collection at issue, then no defense attorney, even one with an appropriate security clearance, would have a "need to know" any of the FISA materials.

Further, Chhipa is not entitled to the FISA materials to bolster his challenge to the lawfulness of the FISA authorities, as FISA's plain language precludes defense counsel from accessing the classified FISA materials to conduct a fishing expedition. In *Medunjanin*, the court noted that "[d]efense counsel . . . may not inspect the FISA dockets to construct a better argument for inspecting the FISA dockets. Such a circular exercise would be patently inconsistent with FISA . . . ." 2012 WL 526428, at *10. *See also Badia*, 827 F.2d at 1464 (rejecting the defendant's request for "disclosure of the FISA application, ostensibly so that he may review it for errors"); *Mubayyid*, 521 F. Supp. 2d at 131 ("The balance struck under FISA . . . would be substantially undermined if criminal defendants were granted a right of disclosure simply to ensure against the possibility of a *Franks* violation.")

Chhipa failed to present any colorable basis for disclosure, as this Court can review and decide the legality of the FISA collection without defense counsel's assistance. Where, as here, defense participation is not necessary, FISA requires that the FISA materials remain protected from disclosure. Congress' clear intention is that FISA materials should be reviewed *in camera* and *ex parte* and in a manner consistent with the realities of modern intelligence needs and investigative techniques. There is nothing extraordinary about this case that would prompt this Court to order the disclosure of highly sensitive and classified FISA materials. *See Rosen*, 447 F. Supp. 2d at 546 (the "exceptional nature of disclosure of FISA material is especially appropriate in light of the possibility that such disclosure might compromise the ability of the United States to gather foreign intelligence information effectively") (citing *Belfield*, 692 F.2d at 147). Accordingly, this Court should deny Chhipa's motion for disclosure under 50 U.S.C. § 1806(f).

2. Due Process Does Not Require Disclosure

Chhipa also failed to establish a basis for disclosure under 50 U.S.C. § 1806(g) and the due process clause. Mot. at 74. As noted earlier, FISA provides that once a district court has concluded

that electronic surveillance and physical search were "lawfully authorized and conducted," "it *shall* deny the motion of the aggrieved person *except to the extent that due process requires discovery or disclosure*." 50 U.S.C. §§ 1806(g), 1825(h) (emphasis added). Courts agree that FISA's *in camera, ex parte* review does not violate the Due Process Clause of the Fifth Amendment, nor does due process require that defendant be granted access to the FISA materials, except as provided for in 50 U.S.C. §§ 1806(f), (g) and 1825(g), (h).[24] Moreover, Chhipa cannot identify any due process violation arising from the application of FISA's review procedures.

The plain intention of 50 U.S.C. §§ 1806(g) and 1825(h)—allowing the Court to order disclosure of material to which the defendant would be entitled under the Due Process Clause, such as material that had not been previously disclosed under *Brady v. Maryland*, 373 U.S. 83 (1963), even while ruling against the defendant's motions generally—cannot be interpreted to support Chhipa's demand for access to all of the FISA materials in advance of the Court's *in camera, ex parte* review and determination of the legality of the collection. Regarding any claim that the FISA materials contain information that due process requires be disclosed to the defense, the request is premature since the Court will determine that itself during its *in camera, ex parte* review. The Government submits that the Court's review of the FISA materials will not reveal any material that due process requires be disclosed to Chhipa, such as *Brady* material, as provided for in 50 U.S.C. §§ 1806(g) and 1825(h). Thus, the provisions concerning due process in 50 U.S.C. §§ 1806(g) and 1825(h) cannot justify disclosure of the FISA materials.

---

[24] *See, e.g.*, *Belfield*, 692 F.2d at 148-49; *El-Mezain*, 664 F.3d at 567; *Abu-Jihaad*, 630 F.3d at 129; *Damrah*, 412 F.3d at 624; *Ott*, 827 F.2d at 476-77; *Nicholson*, 955 F. Supp. at 592 (a judge in this district found, based on "the unanimous holdings of prior case law, . . . that FISA does not violate the Fifth or Sixth Amendments by authorizing *ex parte in camera* review"); *Benkahla*, 437 F. Supp. 2d at 554; *Jayyousi*, 2007 WL 851278, at *7-8; *Falvey*, 540 F. Supp. at 1315-16.

3. This Court Should Deny Chhipa's Motion for Notice Regarding Any Other Surveillance Methods

Chhipa next claims that he is entitled to notice of use of Section 702 and other surveillance programs under the Fourth and Fifth Amendments, 18 U.S.C. § 3504, and the Federal Rules of Criminal Procedure 12 (Rule 12) and 16 (Rule 16). Mot. at 75-78. His motion should be denied because the Government complied with its notice and discovery obligations.

a. Chhipa Is Not Entitled to Section 702 Notice Under FISA

The government's notice obligations regarding the use of FISA information under Section 702 apply if the government (1) "intends to enter into evidence or otherwise use or disclose" (2) "against an aggrieved person" (3) in a "trial, hearing or other proceeding in or before any court, department officer, agency, regulatory body, or other authority of the United States" (4) any "information obtained or derived from" (5) "electronic surveillance of that aggrieved person." 50 U.S.C. §§ 1806(f), 1881e(a) (providing that information acquired pursuant to Sections 702 and 703 of FISA "shall be deemed to be information acquired from electronic surveillance pursuant to" Title I of FISA). When all five criteria are met, the government must provide notice that it intends to use or disclose Section 702 information.

Here, the Government only intends to use as evidence against Chhipa information to which he is an aggrieved person that was obtained or derived from electronic surveillance and physical search conducted pursuant to Title I and III of FISA. Accordingly, the Government complied with its notice obligations when it gave notice of its intent to use information obtained or derived from Title I and Title III of FISA. ECF No. 50. The Government had no reason to provide notice of FISA use under Section 702, and it would be inappropriate to compel "official notice of Section 702" when FISA does not provide for such notice under the circumstances.

b. Chhipa Is Not Entitled to Additional Notice Under the Constitution and Federal Rules of Criminal Procedure

The government's discovery obligations in a criminal case are not limitless. *See United States v. Agurs*, 427 U.S. 97, 106 (1976) (the government is under "no duty to provide defense counsel with unlimited discovery of everything known by the prosecutor"); *United States v. Phillips*, 854 F.2d 273, 277 (7th Cir. 1988) (finding that discovery rules do "not grant criminal defendants unfettered access to government files"); *United States v. Griebel*, 312 F. App'x 93, 96 (10th Cir. 2008) (the government's discovery obligations "are defined by Rule 16, *Brady*, *Giglio*, and the Jencks Act"). There is no rule of discovery that requires the government to provide a defendant with a narrative regarding the origins of the criminal investigation that led to his arrest. *See Pennsylvania v. Ritchie*, 480 U.S. 39, 59 (1987) ("defendant's right to discover exculpatory evidence does not include the unsupervised authority to search through the [government's] files"); *United States v. Bagley*, 473 U.S. 667, 675 (1985) ("the prosecutor is not required to deliver his entire file to defense counsel"). Further, "[n]either the Supreme Court nor [the 10th Circuit] has recognized a due process right to notice of specific techniques the government used to surveil the defendant in a foreign intelligence investigation . . . ." *United States v. Muhtorov*, 20 F.4th 558, 630 (10th Cir. 2021). Rather, the government must provide the defense with all discoverable material (including exculpatory information) described in Rule 16.

Rules 12 and 16 generally govern notice concerning the government's intent to use evidence in a criminal case. Rule 12(b)(4)(B) provides, in relevant part:

> [T]he defendant may, in order to have an opportunity to move to suppress evidence under Rule 12(b)(3)(C), request notice of the government's intent to use (in its evidence-in-chief at trial) any evidence that the defendant may be entitled to discover under Rule 16.

The purpose of this rule is to "provide the defendant with sufficient information to file the necessary suppression motions." *United States v. Ishak*, 277 F.R.D. 156, 158 (E.D. Va. 2011) (internal quotation marks and citation omitted). "Thus, the government's obligation under Rule 12(b)(4)(B) ends when it has made disclosures that sufficiently allow the defendants to make informed decisions whether to file one or more motions to suppress." *Id.*

In the context of FISA collection, Congress allowed for greater protection of information than is normally afforded because of the need to protect sensitive national security information, which includes classified sources and methods. Congress intended that FISA "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." S. Rep. No. 95-701, at 16, 1978 U.S.C.C.A.N., at 3985. As such, in recognition of "the nature of the national interests implicated in matters involving a foreign power or its agents," Congress provided for more limited disclosure than is ordinarily provided for criminal defense. *Belfield*, 692 F.2d at 148.

Here, the Government has satisfied its notice obligations and provided Chhipa with enough information and notice to file any necessary motions to suppress. No court has interpreted Rules 12 and 16 to require the government to describe every investigative technique used in the case, regardless of its relationship to admissible evidence. Indeed, Congress "intentionally replaced [Rules 12 and 16] with FISA's disclosure framework" and rendered Rule 16 and other existing laws inapplicable to discovery in the FISA context. *Aziz*, 228 F. Supp. 3d at 370 (citing *Thomson*, 752 F. Supp. at 82; *Spanjol*, 720 F. Supp. at 59.) "Rules 12 and 16 do not, and cannot, supersede FISA's statutory prohibition on disclosure," *Aziz*, 228 F. Supp. 3d at

370, and thus this Court should deny Chhipa's request for more information than is legally required.[25]

Chhipa's contention that he is entitled to enhanced notice is further refuted by Congress's assignment of broader FISA notice requirements in certain circumstances, not to include in the context of criminal defendants. *See Dean v. United States*, 556 U.S. 568, 573 (2009) ("[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."). Specifically, Congress identified three scenarios where more specific notice regarding FISA surveillance was warranted. *See* 50 U.S.C. § 1806(j) (notice of particular information regarding surveillance required where the Attorney General approves emergency surveillance and the government does not later obtain authorization from the FISC); *id.* § 1825(b) (requiring notice identifying property seized, altered, or reproduced during physical search of a U.S. person's residence where the Attorney General has determined that there is no national security interest in continued secrecy); *id.* § 1825(j) (notice of particular information regarding physical search required where the Attorney General approves emergency physical search and the government does not later obtain authorization from the FISC). Congress elected not to require such broad disclosure in the situation where a defendant is charged in a criminal

[25] Chhipa cites to *United States v. Soto-Zuniga*, 837 F.3d 992, 1000-01 (9th Cir. 2016), in support of his statement that he is entitled to notice of the government's surveillance techniques because the information is "material" under Rule 16. Mot. at 78. In *Soto-Zuniga*, the Ninth Circuit held that the defendant was entitled to discovery of specified information to support the defendant's motion challenging the constitutionality of a border checkpoint search. 837 F.3d at 1002. But *Soto-Zuniga* is an out-of-circuit case that did not involve FISA, and thus it is not probative.

proceeding. *See* 50 U.S.C. §§ 1806(c) and 1825(d) (requiring only notice "that the United States intends" to use or disclose FISA-obtained or -derived information).

c. Chhipa Is Not Entitled to Additional Notice Under 18 U.S.C. § 3504

Chhipa next argues that he is entitled to additional notice and discovery under 18 U.S.C. § 3504. Mot. at 77-78. That section provides, in relevant part:

> In any trial, hearing, or other proceeding in or before any court . . . [u]pon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act.

18 U.S.C. § 3504 is inapplicable because Chhipa did not establish a colorable basis that any unlawful surveillance has aggrieved him. *See Muhtorov*, 20 F.4th 558 at 631 (finding a defendant's general, unsupported allegations of unlawful acts were insufficient to trigger the government's obligation to confirm or deny the use of surveillance techniques under 18 U.S.C. § 3504); *see also United States v. Osadzinksi*, No. 19 CR869, 2021 WL 3209671, at *6 (N.D. Ill July 29, 2021) (holding the government need not give notice under 18 U.S.C. § 3504 when "defendant has not provided any allegations regarding an unlawful act, let alone any basis for such an allegation"), *aff'd*, 97 F.4th 484 (7th Cir. 2024). Moreover, the FISA information did not spring from an unlawful act; it was lawfully obtained pursuant to FISC order(s). *See Muhtorov*, 20 F.4th 558 at 631 (finding "the government's denial that any evidence was derived from" alleged illegal surveillance was "sufficient to carry its burden under § 3504.")

The Government provided the notice required under the FISA statute. No court has held that in addition to 50 U.S.C. §§ 1806(c) or 1825(d), the government has an additional notice requirement under 18 U.S.C. § 3504. Indeed, "FISA's particularized notice, disclosure, and suppression procedures supplant the requirements of § 3504." *Aziz*, 228 F. Supp. 3d at 370.

A specific statutory provision normally controls over one of more general application. *See Bloate v. United States*, 559 U.S. 196, 207-08 (2010). Moreover, 50 U.S.C. §§ 1806(c) and 1825(d) were enacted in 1978 and 1994, respectively, about eight and 24 years after 18 U.S.C. § 3504 was adopted in 1970. *See* Organized Crime Control Act of 1970, Pub. L. No. 91-452, § 702, 84 State. 922, 935-36 (1970). "[A] later enacted statute may limit the scope of an earlier statute." *Bhd. of Maintenance of Way Emps. v. CSX Transp., Inc.*, 478 F.3d 814, 817 (7th Cir. 2007). There is no basis for holding that 18 U.S.C. § 3504 trumps FISA's "later-enacted, more specific" notice provisions. Thus, this Court should deny Chhipa's motion for additional notice.

4. The Adversary System Does Not Require Disclosure

Chhipa next claims that the adversary system requires disclosure of the FISA materials, and that *ex parte* proceedings are antithetical to the adversary legal system. Mot. at 81-89. This claim is contrary to relevant case law. As the Fourth Circuit stated, "Congress did not run afoul of the Constitution when it reasoned that the additional benefit of an unconditional adversarial process was outweighed by the Nation's interest in protecting itself from foreign threats." *Dhirane*, 896 F.3d at 301; *see also Falvey*, 540 F. Supp. at 1315-16 (rejecting First, Fifth, and Sixth Amendment challenges and noting that a "massive body of pre-FISA case law of the Supreme Court, [the Second] Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an *in camera*, *ex parte* basis).

Moreover, *ex parte* proceedings are not foreign to the American criminal justice system. *See Daoud*, 755 F.3d at 482; *see also Isa*, 923 F.2d at 1307. Courts have consistently rejected similar arguments challenging FISA under the Sixth Amendment. *See Belfield*, 692 F.2d at 148-49; *Isa*, 923 F.2d at 1306-07; *Warsame*, 547 F. Supp. 2d at 988 n.4 (citing *Nicholson*, 955 F. Supp. at 592); *Megahey*, 553 F. Supp. at 1193. Indeed, in overturning a district court's order to

disclose FISA materials to the defense, the Seventh Circuit in *Daoud* described the belief that "adversary procedure is always essential to resolve contested issues of fact" as "an incomplete description of the American legal system in general and the federal judicial system in particular." 755 F.3d at 482. This Court should likewise reject Chhipa's challenge.

D. CIPA Does Not Violate Due Process

Finally, Chhipa alleges that the Government concealed, is concealing, or will conceal surveillance techniques through its Section 4 filing under the Classified Information Procedures Act (CIPA), 18 U.S.C. App. 3. *Id.* at 78-81. However, the Government properly followed CIPA's procedural framework in filing its CIPA Section 4 motion – a framework consistently found to preserve defendants' due process rights while remaining protective of national security interests. *See United States v. Kotey*, 545 F. Supp. 3d 331, 337 (E.D. Va. 2021) (". . . any Fifth Amendment Due Process right is limited to material within the realm of *Brady* and its progeny, and is effectively protected by the procedures set forth under CIPA § 4."); *United States v. Moussaoui*, 591 F.3d 263, 282 (4th Cir. 2010) ("CIPA provides procedures for protecting classified information without running afoul of a defendant's right to a fair trial"); *United States v. Mejia*, 448 F.3d 436, 458 (D.C. Cir. 2006) (upholding constitutionality of *ex parte* CIPA proceedings).

[CLASSIFIED INFORMATION REDACTED]

VI. CONCLUSION: THERE IS NO BASIS TO DISCLOSE THE FISA MATERIALS OR SUPPRESS THE FISA INFORMATION

Based on the foregoing analysis, the Government submits that the Court must conduct an *in camera*, *ex parte* review of the FISA materials and the Government's classified submissions, and should: (1) find that disclosure of the FISA materials and the Government's classified submissions to Chhipa is not authorized because the Court is able to make an accurate

determination of the legality of the surveillance and searches without disclosure; (2) find that the electronic surveillance and physical search at issue were both lawfully authorized and conducted in compliance with FISA; (3) hold that the fruits of the electronic surveillance and physical search should not be suppressed; and (4) order that the FISA materials and the Government's classified submissions be maintained under seal by the Classified Information Security Officer or his or her designee.[26]

Respectfully submitted,

JESSICA D. ABER
United States Attorney

/s/
Anthony T. Aminoff
Amanda St. Cyr
Assistant U.S. Attorneys
United States Attorney's Office
Eastern District of Virginia

Andrew J. Dixon
Andrea Broach
Trial Attorneys
DOJ National Security Division
Counterterrorism Section

Date: August 30, 2024

[26] A district court order granting motions or requests under 50 U.S.C. §§ 1806(g) or 1825(h), a decision that electronic surveillance or physical search was not lawfully authorized or conducted, and an order requiring the disclosure of FISA materials are each a final order for purposes of appeal. *See* 50 U.S.C. §§ 1806(h), 1825(i). Should the Court conclude that disclosure of any item within any of the FISA materials or suppression of any FISA-obtained or -derived information may be required, given the significant national security consequences that would result from such disclosure or suppression, the Government would expect to pursue an appeal. Accordingly, the Government respectfully requests the Court stay any such order pending an appeal by the United States of that order.